Datenschutz-Awareness umsetzen

Der DSB: Freund oder Feind?

Datenschutz is here to stay, wie Steuern und Tempolimits. Viele Forderungen der DSGVO sind schon seit den 1980er Jahren Gesetz, und das Thema Privacy by Design wurde unter dem etwas unglücklichen Begriff „Datensparsamkeit“ in BDSG §3a aufgeführt. Wir brauchen einen vertrauensvollen Austausch der Entwickler, Fachbereiche und Datenschutzbeauftragten (DSB), um Ideen und Projektansätze frühzeitig zu prüfen, zu argumentieren und anzupassen. Wir müssen über eine generelle Datenschutz-Awareness nachdenken und eine Change Facilitation bei den Beteiligten aufsetzen.

von Rolf Scheuch

Wir haben den Artikel etwas reißerisch betitelt, da viele Entwickler und Product Owner aus den Fachbereichen den Datenschutzbeauftragten (DSB) leider oft als Bremser, Bedenkenträger oder schlicht Neinsager wahrnehmen und ihn so in eine Verteidigungsposition drängen. Dies sollte und darf aber nicht so sein. Der DSB hat laut DSGVO keine Weisungsbefugnis, sondern seine Aufgabe besteht darin, auf die Einhaltung der Gesetze und Richtlinien hinzuwirken. Gerade die private Nutzung sozialer Netzwerke führt bei vielen von uns zu einem eigenen, privaten Anspruch an den Datenschutz von personenbezogenen Daten. Oft führte das bereits zu einer Desillusion und dem Grundgefühl, dass der Kampf um den Datenschutz bereits verloren sei. Facebook, Google, Amazon und andere Datenkraken überraschen uns immer wieder mit Skandalen, die uns den fehlenden Schutz personenbezogener Daten vor Augen führen.

Können wir diese Laissez-faire-Haltung aus unserem privaten Umfeld auch im Wirtschaftsleben beibehalten? Leider nein, denn zu eindeutig sind die gesetzlichen Regularien und industrie- bzw. unternehmensspezifischen Compliance-Auflagen. Ob diese im Einzelfall sinnvoll sind, darüber lässt sich am Stammtisch vortrefflich streiten, jedoch ist eine Diskussion über Sinn und Zweck im Unternehmen nicht zielführend. Somit ist eine Diskrepanz zwischen eigenem, privaten Anspruch und einer geschäftlichen Sichtweise im Unternehmen zwar vorhanden, darf aber nicht zu einem Fehlverhalten beim wirtschaftlichen Handeln führen. Der Datenschutz steht vor dem Problem, dass jeder Mensch eine unterschiedliche Vorstellung hat, was Privatsphäre bedeutet. Die Gesetze sind so formuliert, dass jeder mehr preisgeben kann, wenn er möchte, aber eben auch die geschützt sind, die es nicht möchten. Die Unternehmen und Organisationen müssen diejenigen berücksichtigen, die weniger von sich preisgeben möchten. Mithilfe von vier Beispiele aus unserem Unternehmen möchten wir die notwendige Zusammenarbeit mit dem DSB deutlich machen und zu einem partnerschaftlichen Umgang motivieren.

Chatbots sind die Zukunft I

Im Zuge unserer digitalen Transformation zu einer Digitalen Service Manufaktur [1] ist eine Kommunikation der Sinnhaftigkeit und von erreichten Erfolgen ein wichtiges Mittel, um alle im Unternehmen mitzunehmen. Hierzu haben wir ein DIN-A2-Poster mit Projekten, die uns mit Stolz erfüllen, als eine Art Wimmelbild [2] erstellt und hierzu auch entsprechende Texte für ein Storytelling erstellt. Wie vermittelt man diese Erfolgsgeschichten etwas lockerer und leichter? Hier hatten wir die die Idee, die Stories im Dialog mit dem Chatbot Alexa erzählen zu lassen. In den Kaffeeküchen sollten Chatbots aufgestellt werden, und man konnte in zwangloser Atmosphäre Alexa bitten, eine Story zu erzählen. Nachdem wir dies implementiert, getestet und rundgeschliffen hatten, hat der DSB per Zufall davon erfahren. Neugierig hat er es getestet und, da er selbst auch Entwickler ist, hat er sich tiefergehend informiert.

Hierbei wurde deutlich, dass Alexa stets, auch im Ruhezustand, die Gespräche aufnimmt und zur Analyse an Amazon überträgt [3]. An dieser Stelle hat der DSB empfohlen, das Projekt zu stoppen und nicht breitflächig einzuführen, da die Privatsphäre und die Datensicherheit personenbezogener Daten wie auch möglicher Kundeninformationen in den Kaffeeküchengesprächen nicht mehr gesichert sind. Laut der AGB von Amazon darf Alexa lediglich für den privaten, nichtkommerziellen Gebrauch verwendet werden.

Ein Bot bereitet Wissen auf I

Ein weiteres internes Projekt zur Effizienzsteigerung bezieht sich auf das Wissensmanagement. Ein Bot, ein Roboter, unterstützt bei einer intelligenten Suche, um zu technischen oder fachlichen Stichworten die Know-how-Träger vorzuschlagen. Diese Könner kann man sodann kontaktieren und um Hilfe zu bitten, um seine Herausforderung zu meistern. Hierzu wurden alle relevanten Dokumente, technische Forumseinträge und Erläuterungen zu den Zeitaufschreibungen in einen Data Lake extrahiert und über einen intelligenten Ranking-Mechanismus bewertet, um den besten Ansprechpartner vorzuschlagen. Das System wurde mit einem klassischen Open Source Stack für Big Data realisiert und lieferte bereits in der Testphase gute, zum Teil überraschende Erkenntnisse. Vor dem Ausrollen wurde das System dem DSB präsentiert, und er bemängelte das Ranking, da es eine implizite Bewertung der Fähigkeiten von Mitarbeitern darstelle. Der wirtschaftliche Zweck der Lösung war ihm einleuchtend und er sah ihn für das Unternehmen durchaus positiv, aber wegen des Rankings wurde das Projekt „Guru“ erst einmal auf Eis gelegt.

Anhand dieser beiden Beispiele zeichnet sich bereits ein Muster ab. Der DSB wird oft einfach zu spät eingebunden bzw. das Quality Gate für die Bewertung des Datenschutzes erfolgt zu spät. In den beiden vorhergehenden Artikeln dieses Magazins wird deshalb auch so viel Wert auf Privacy by Design gelegt.

Die Geburtstagsliste I

Eine der vielen kleinen und guten Ideen ist die Nutzung einer Geburtstagsliste, um Mitarbeitern zum richtigen Termin zu gratulieren bzw. mehrere Geburtstagskinder zu einer kleinen Party zusammenzufassen. Dies sollte über eine Geburtstagsliste und Push Notifications an den Vorgesetzten realisiert werden. Die HR-Abteilung fand die Idee ebenfalls gut und hat von sich aus den DSB hinzugezogen. Nachdem er sich informiert hatte, bat er uns, den wirtschaftlichen Zweck genauer zu formulieren und eine Begründung zu geben, warum eine Angabe des Geburtsjahres wichtig ist.

User Experience über mobile Apps I

Ähnlich wie viele unserer Mandanten, haben auch wir in nunmehr achtundzwanzig Jahren Tätigkeit eine Sammlung an Legacy-Anwendungen für Projektabwicklung und -abrechnung sowie ein individuelles CRM-System. Zur Ermöglichung einer mobilen Nutzung wollten wir für relevante Use Cases Apps erstellen, die ein mobiles Arbeiten mit einer guten User Experience ermöglichten. Hierzu haben wir die Altsysteme sukzessive über einen API-First-Ansatz mit Businessservices gekapselt und entsprechende Apps erstellt. Damit User Experience und Performance optimiert werden konnten, haben wir viele, auch personenbezogene Daten in einem Cache gehalten. Dies hat unser DSB bemängelt und empfohlen, die Architektur zu überdenken.

Bevor wir uns unsere Beispiele und die Lösung der damit verbundenen Probleme genauer anschauen, gehen wir zunächst ein wenig näher auf die Rolle des DSB und insbesondere auf seine Aufgaben ein. Die aufgeführten Beispiele zeigten, dass wir etwas falsch gemacht haben bzw. die Rolle des DSB in der Organisation nicht richtig gelebt und die Expertise des DSB in den Projekten nicht ausreichend einbezogen wurde.

Rolle und Aufgaben des Datenschutzbeauftragten

Wer wann und ob man überhaupt einen DSB bestellen muss, ist in Artikel 37 Abschnitt 1 der DSGVO nachzulesen. Unser Schwerpunkt liegt auf den Aufgaben des DSB, seiner Rolle und konkret dem Zusammenspiel mit Entwicklern. Der DSB soll letztlich dafür Sorge tragen, dass die datenschutzrechtlichen Bestimmungen, auch bezüglich des Umgangs mit personenbezogenen Daten, in den Projekten bzw. Applikationen eingehalten werden. Die Rolle des DSB ist sehr weit gefasst und die Aufgabe ist situativ, weshalb wir es als schwierig bis hin zu kontraproduktiv halten, ein klassisches Rollenbild mit Prozessen zu beschreiben. Vielmehr bietet es sich an, die Anforderungen an den DSB als Leitlinien für sein Handeln aufzufassen und somit den Handlungsspielraum zu vergrößern.

Schon immer durften personenbezogene Daten nur dann verarbeitet werden, wenn ein (Geschäfts-)Grund angegeben wurde. Ein einleuchtendes Beispiel ist die Fakturierung bzw. der Versand von Waren, wobei eine persönliche Adresse verwendet werden muss. Die neue Erlaubnis nach Artikel 6 (f) ist sogar weitreichender. Es genügt jetzt schon „berechtigtes Interesse“ mit Abwägung der „Grundrechte und -freiheiten“ der Betroffenen. Dieses Spannungsfeld ist ein Aufgabengebiet des DSB. Die neue DSGVO hat hierzu zwei Begriffe eingeführt: den des Verantwortlichen und den des Auftragsverarbeiters.

Nach Art. 4 Z 7 DSGVO ist ein „Verantwortlicher“ eine natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Und nach Art. 4 Z 8 DSGVO ist ein „Auftragsverarbeiter“ eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet. Hierbei ist der Auftragsverarbeiter eine andere Stelle als der Verantwortliche, der die Daten verarbeitet. Einige Bespiele des Unterschieds von Auftragsverarbeiter und Verantwortlicher sind: Der Cloud-

Provider als Auftragsverarbeiter bei Back-ups, ein ausgelagerter Rechnungssteller, wie etwa die DATEV, die Durchführung von Kundenkontakten durch externe Callcenter oder Ähnliches. Wir selbst sind als Managed Service Provider und XaaS-Anbieter in der Regel auch selbst der Auftragsverarbeiter für unsere Kunden.

Wenden wir diese Sicht nun auf meinen Facebook-Account an. Mein Vertrag als natürliche Person erfolgt direkt mit Facebook über deren Website, sodass ich der Kunde bin. Facebook ist somit der Auftragsbearbeiter meines Social-Media-Accounts, und ich habe als Verantwortlicher über einen Nutzungsvertrag den Zweck gebilligt. Hieraus ergeben sich laut DSGVO die Betroffenenrechte als Verantwortlicher, die Haftung des Auftragsverarbeiters sowie dessen Verantwortlichkeit für technische organisatorische Sicherheitsmaßnahmen und Dokumentationspflichten, wie etwa Verzeichnis der Verarbeitungstätigkeiten, Datenschutzfolge-Abschätzung und Nachweispflichten.

Wir möchten die grundlegenden Anforderungen aus der DSGVO in eine Top-down- und eine Bottom-up-Sicht unterscheiden. Bei der Top-down-Sicht wollen wir alle grundlegenden Anforderungen zusammenfassen, die unabhängig von einem Einzelfall erfolgen und sich im Management einer internen Datenschutzorganisation zusammenfassen. Bottom-up sind die situativen, oft beratenden Aufgaben, die sich auf Eskalationen und die Beschäftigung mit Einzelfällen, etwa einer Vorabkontrolle oder Risikoabschätzung eines Projekts, beziehen.

Top-down

Aufgabe ist die Optimierung der technischen und organisatorischen Abläufe für ein Management des Datenschutzes. Gerade bei größeren Organisationen ist es offensichtlich, dass ein DSB auf verlorenem Posten ist. Hier ist es die Aufgabe, eine funktionierende Organisation aufzubauen und Mitarbeiter für das Thema Datenschutz zu sensibilisieren. Eine Datenschutzorganisation lässt sich letztlich als eine Governance-Organisation auffassen, wobei die Verantwortung und Haftung bei der Geschäftsführung liegt. Der DSB leitet diese meist virtuelle Organisation als Stabsstelle unter der Geschäftsführung und regt die relevanten – und letztlich somit fast alle – Fachbereiche an, die notwendige Sorgfalt walten zu lassen. Ferner wirkt der DSB darauf ein, die Mitarbeiter für das Thema Datenschutz zu sensibilisieren, etwa durch Schulungs- und Kommunikationsmaßnahmen. Dies ist letztlich ein Wandlungsprozess, der seitens der Geschäftsführung mithilfe des DSB angestoßen und von den Fachbereichen durchgeführt wird. Hierzu gehören Weiterbildungsmaßnahmen, etwa Schulungen, oder auch Change-Facilitation-Maßnahmen.

Die Qualifizierung und Awareness für Datenschutz für die verantwortliche Stelle ist eine gemeinschaftliche Top-down-Aufgabe, der DSB überwacht nur die Durchführung.

Die gesetzliche Auflage der „Verantwortung der verarbeitenden Stelle“ ist ohne eine aktive Mitwirkung der Fachbereiche, wobei wir die IT als eigenen Fachbereich betrachten, kaum möglich. Somit ist die aktive Mitarbeit der Fachbereiche letztlich entscheidend, damit Datenschutz aktiv gelebt und nicht verwaltet wird. Die Organisation wird jedoch seitens des DSGVO einige harte Regularien erfüllen müssen. Dies sind Funktionen im Verhältnis zu den Aufsichtsbehörden wie auch die Implementierung einer gesetzlich vorgeschriebenen Anlaufstelle von internen wie auch externen Betroffenen. Die DSGVO erwartet seitens der Datenschutzorganisation eine Kontrollfunktion hinsichtlich der datenschutzrechtlichen Erfordernisse [4] bei der Verarbeitung, Speicherung und Kommunikation von personenbezogenen Daten und die nicht näher erläuterte Vorabkontrolle.

Der DSB mit seiner Organisation agiert als unabhängiges Kontrollorgan und prüft regelmäßig die Arbeitsabläufe, um den Datenschutz im Unternehmen zu gewährleisten. Stellt er Verstöße fest, muss er sie der Geschäftsführung melden und gemeinsam mit ihr bewerten, um entsprechend Risiken zu identifizieren, zu bewerten und geeignete Initiativen zu ergreifen. Zusammengefasst sehen wir vier unterschiedliche Bereiche, in denen die DSGVO Vorgaben macht: den Aufbau einer Datenschutzorganisation, die Nutzung von Technologie zum Datenschutz, die Implementierung von internen Prozessen und Verfahren und die Ermöglichung einer Nachweisbarkeit und Dokumentation der rechtlichen Vorgaben. Das bereitet schnell Kopfzerbrechen, wie auch aus den Beispielen ersichtlich. Wann wird der DSB hinzugezogen? Wann erfährt die Datenschutzorganisation von Projekten mit Verarbeitung personenbezogener Daten? Sobald man diese Anforderung als „klassisches“ Quality Gate in einem Freigabeprozess lebt, Datenschutz nur verwaltet und eine Ex-post-Bewertung des DSB einholt, treten die in den Beispielen oben dargestellten Probleme auf. Wie sollte man praktisch vorgehen? Was können Entwickler tun, um den DSB einzubinden und seine Expertise zu nutzen?

Bottom-up

Hier hilft eine Bottom-up-Sichtweise weiter. Entsprechend qualifizierte Lösungsarchitekten werden schon bei der Projektskizze bzw. dem Design der Lösung aufgefordert, den Zweck der Nutzung der personenbezogenen Daten zu erläutern, die personenbezogenen Daten auf die Nutzung zu analysieren und eine Vorabprüfung vorzunehmen. Der qualifizierte Lösungsarchitekt kann der DSB selbst sein oder entsprechend qualifizierte Mitarbeiter, um die Menge an relevanten Anfragen überhaupt bewältigen zu können. Dies sollte keinen größeren Aufwand darstellen, da es bei Projekten, auch im agilen Umfeld, üblich ist, nichtfunktionale Anforderungen zu prüfen. Der Datenschutz wäre somit eine weitere nichtfunktionale Anforderung. Im ersten Artikel hatten wir die Notwendigkeit von Privacy by Design erläutert und vorgestellt, wie diese Sichtweise beim Architekturentwurf einfließt.

Reload der Projekte

Auf Basis der durchgeführten Retrospektiven bei den beschriebenen Projekten wurde ein Reload der Projekte mit dem DSB beschlossen. Als Vorbereitung auf eine Beratung des DSB und den Versuch einer DSGVO-konformen Lösungsfindung haben wir unsere Hausaufgaben gemacht. Der wirtschaftliche Zweck der Nutzung der personenbezogenen Daten wurde genauer ausgeführt und insbesondere ein Katalog der personenbezogenen Daten pro Anwendung bzw. Projekt aufgeführt und die Bedeutung der Attribute erläutert. Die Erfahrung zeigte uns, dass dies nicht allzu aufwendig war, da die Menge an notwendigen personenbezogenen Attributen meist bei unter fünf lag.

Chatbots sind die Zukunft II

Als Auftragsbearbeiter der Sprachinformationen wurde Amazon als Betreiber der Alexa-Plattform identifiziert, und wir haben unsere Anforderungen als Verantwortliche festgehalten. Die Forderung der unmittelbaren Löschung der Daten, die keine Alexa-Anfrage waren, durch Amazon war nötig, um einen weitreichenden Einsatz zu ermöglichen. Zum einen mussten wir Rechte der Mitarbeiter an ihren Gesprächen schützen wie auch die Pflichten des Unternehmens gegenüber unseren Kunden erfüllen, die in Gesprächen erwähnt werden konnten. Gespräche mit Amazon zeigten schnell auf, dass diese Forderung nach unmittelbarer Löschung von Amazon nicht akzeptiert werden würde. Somit wurde das Chatbot-Experiment gestoppt.

Ein Bot bereitet Wissen auf II

Die Verantwortlichen waren unsere Mitarbeiter mit dem Wunsch nach einer Unterstützung bei der Suche nach einem Spezialisten und der gleichzeitigen Anforderung, nicht bezüglich ihres Outputs über ein Ranking bewertet zu werden. Hier haben wir mit dem DSB eine Lösung entworfen, die auf ein Ranking verzichtet und

dem Fragesteller selbst am Bildschirm die Gelegenheit bietet, die Inhalte zu sichten und für sich das Passende zu finden. Hier haben wir uns auch gegen ein implizites Ranking über Likes etc. entschieden. Somit war ein Reload des Projekts möglich.

Die Geburtstagsliste II

Dieses kleine Projekt war schnell gelöst. Keiner der Stakeholder hatte ein Interesse am Alter des Mitarbeiters, sondern nur an seinem Geburtsdatum. HR untermauerten die Verbesserung der Mitarbeiterbindung als Zweck dieser Maßnahme. Da auch seitens des Mitarbeiters keine Nachteile ersichtlich waren, war ein Reload des Projekts möglich.

User Experience über mobile Apps II

Durch die Nutzung personenbezogener Daten in den mobilen Apps war in diesem Fall eine intensive Auseinandersetzung mit der Applikationsarchitektur notwendig. Der Zweck als wirtschaftliche Notwendigkeit war nicht Gegenstand der Diskussion, da insbesondere für die Mitarbeiter eine Arbeitserleichterung bei den formal notwendigen Datenerfassungen erfolgt und ein berechtigtes Interesse der verarbeitenden Stelle vorlag. Die aktuelle technische Implementierung ermöglichte jedoch eine Verletzung des Datenschutzes durch die redundante Speicherung jenseits der Firewall. Über ein neues API-Konzept mit einer verstärkten Datenaufbereitung in einem gesicherten Backend for Frontend war es möglich, diesen Schwachpunkt zu umgehen. Ein Prototyp ermöglichte eine detaillierte Überprüfung der Sicherheitsaspekte. Somit war auch in diesem Fall ein Reload der Apps-Projekte mit einem API-Ansatz umsetzbar.

Big-Data-Ansätze und Zweckbindung

Big-Data-Ansätze haben ein inhärentes Problem: Die Zweckbindung. In Artikel 5 der DSGVO wird gefordert, dass die Daten für „festgelegte, eindeutige und legitime Zwecke“ erhoben und später nicht „in einer mit diesen Zwecken nicht zu vereinbarenden Weise“ weiterverarbeitet werden. Ein Beispiel: Wenn ich ein Gewinnspiel mache, muss ich zu Anfang erläutern, dass ich die Teilnehmer auch zu Werbezwecken kontaktieren werde. Im Nachhinein darf ich dies nicht tun. Das macht allerdings Big Data mit kundendatenbezogenen Fragestellungen schwer. Oft ist es im Vorfeld der explorativen Analysen nicht ersichtlich, welche Informationen man aus den Daten gewinnen kann. Dies bedeutet aber auch, dass neue wirtschaftliche Zwecke möglich werden können. Laut der DSGVO muss ich mir vor der Erhebung Gedanken machen, warum ich welche Daten erhebe, ich muss also den Zweck der Datensammlung erläutern. Es ist nicht erlaubt, alle Daten inklusive der personenbezogenen Daten in einen Topf eines Data Lake zu werfen, umzurühren und anschließend die Erkenntnisse etwa für ein 1:1-Marketing zu verwenden, zumindest nicht ohne eine sinnvolle Begründung im Vorfeld mit der entsprechenden Information an den Verantwortlichen.

Fazit

Neben der Notwendigkeit eines Top-down-Ansatzes zur Etablierung einer Datenschutzorganisation mit den geforderten Funktionalitäten und Möglichkeiten eines Nachweises ist ein kooperativer Bottom-up-Ansatz mit einer beratenden Datenschutzorganisation notwendig. Die Form der Implementierung hängt vom Volumen der Anfragen und der räumlichen Verteilung ab, jedoch empfehlen wir, die Expertise des DSB als Berater zu nutzen. Die beratende Funktion ist auch im Gesetz verankert: DSGVO Art. 39 (1a) erläutert die „Beratung des Verantwortlichen“ und DSGVO Art. 39 (1c) spricht von „Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung“.

Wir haben ausführlich dargelegt, dass dies nicht der DSB allein durchführen muss, sondern die verantwortliche Stelle. Die Qualifizierung und Awareness für Datenschutz für die verantwortliche Stelle ist eine gemeinschaftliche Top-down-Aufgabe, der DSB überwacht nur die Durchführung. Hierbei nutzt ein Projektteam die fachliche Kompetenz des DSB bzw. der verantwortlichen Stelle, um bereits beim Projektentwurf bzw. Lösungsdesign die Aspekte des Datenschutzes einzubeziehen. An dieser Stelle helfen selbstverständlich die in den vorhergehenden beiden Artikeln erläuterten Prinzipien beim Privacy by Design weiter. Gerade die steigende Dezentralität der IT und die Autonomie vieler Fachbereiche bei IT-Entscheidungen erfordert eine Datenschutz-Awareness. Damit dies möglich wird, müssen wir, analog einer Digital Awareness, auch eine Datenschutz-Awareness durch geeignete Change-Facilitation-Initiativen umsetzen.

Rolf Scheuch ist Diplom-Mathematiker und hat 1990 das IT-Beratungshaus OPITZ CONSULTING mitbegründet. Dort verantwortete er viele Jahre die Bereiche Business Development und Marketing. Seit 2011 ist er Chief Strategy Officer der Unternehmensgruppe. Heute arbeitet er zudem als Management-Coach und als Autor diverser Bücher und Publikationen zu Themenbereichen wie BPM, SOA oder BI/Analytics.

Links & Literatur

[1] Digitale Service Manufaktur: https://digitale-service-manufaktur.de/

[2] Storytelling als Wimmelbild: https://www.youtube.com/watch?v=ouDCQeVIrZs

[3] verbraucherzentrale.de: „Amazon hört zu: "Echo" jetzt auch in hiesigen Wohnzimmern“. https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/datenschutz/amazon-hoert-zu-echo-jetzt-auch-in-hiesigen-wohnzimmern-13149

[4] Die Bundesbeauftragte für Datenschutz und die Informationsfreiheit: „Info 6: EU-Datenschutz-Grundverordnung“: https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?__blob=publicationFile&v=49